LIBERTY UNIVERSITY

Journal of Fundamental & Applied Business Research

Volume 1 | Issue 1 Article 5

2023

Impact of Cybersecurity Investments on Smaller Organizations

Stephen Mancini

Stephen Mancini

Doctor of Business Administration (Information Systems) / 2022

Applied Research

Impact of Cybersecurity Investments on Smaller Organizations

Abstract

The challenges of securing an organization from various cyber threats are well known. However, it is particularly challenging for smaller organizations to secure themselves due to an often-perceived limitation on funding, and there exists no clear methodology for how an organization should invest the resources it does have. Furthermore, the need to secure oneself is predicated upon an understanding of the threat actors and their methods. This also presents a further challenge as to what information is needed and how to effectively share said information among organizations to understand the threats and threat actors. The following study demonstrated while there exists no clear methodology for cyber investment, nor does there exist a clear process for how best to share cyber-threat intelligence, a smaller organization with limited funds and personnel was able to demonstrate that it is possible for smaller organizations to secure themselves through directed and methodical actions. The study was conducted via interviews over a 2-week period and solicited input from all levels of the organization. The interviews focused on a variety of topics ranging from awareness to local policies to knowledge of recent cyber events. Ultimately, the analysis of the organizational responses revealed several key themes, mainly that a smaller organization could secure itself despite limited resources because its organizational leadership was able to set the tone.

Key words: information sharing, cyber investments, threat actors, cyber policies

Introduction

The following discusses the results of a study which attempts to add to a greater understanding of the challenge organizations, specifically smaller ones, face in attempting to ascertain what constitutes an acceptable amount of investiture into its defensive posture. To begin, there appears to be no general agreement as to what a 'best practice' is in determining acceptable security investment amounts, nor has there been much clarity given on the challenges of defining and understanding the complexity of ascertaining a return on investment for something which yields no outward profit. In other words, why invest in what may be seen as a zero-sum game? Another concern is an organization may never be breached but could be spending far beyond what is necessary to achieve such security; likewise, an organization could be spending appropriately yet still be breached due to the sophistication of the threat actor which begs the question, if the organization invests in its security but is still likely to be breached, why invest much at all? Furthermore, what constitutes a correct amount in either case? While these remain challenges for organizations to ascertain, nonetheless, the study showed a smaller organization with lesser available funding and a smaller staff was still able to secure itself over a 24-month period from any successful cyberattacks. This study leverages a single case study of a smaller organization to define some acceptable understanding as to what potentially constitutes effective approaches to cybersecurity.

Background of the Problem

In 2013, Target Corporation suffered a cyber-attack wherein the final cost was estimated to be $200 million, with an additional commitment of $100 million to upgrade their IT infrastructure (Garg, 2020). A simple reality is that many organizations could not afford these costs. The problem of breaches and information sharing is particularly poignant among small- to

medium-sized organizations (Raineri & Fudge, 2019). Their biggest challenge is often based on funding, which obviously limits the tools and personnel available to mitigate or respond to any threats (Raineri & Fudge, 2019). A survey compiled by Deloitte and the National Association of State Chief Information Officers (NASCIO) showed "75.5% of CISOs cited lack of sufficient budget as a top challenge" (Fielder et al., 2016, p. 13). Fielder et al. (2016) also noted how many subject matter experts highlighted how limited funding in cybersecurity creates a lack of mechanisms available for defense. Coupled with limited resources, smaller organizations suffer from an ineffectual or non-existent process for sharing various types of cyber threat information.

The importance of sharing cyber threat information between organizations, regardless of size, cannot be overstated. In 1998, President Clinton signed the first Presidential Decision Directive to establish an information agreement between the public and private sector (He et al., 2018). Since its signing well over 20 years ago, challenges still exist. For example, while there exists various groups and data formats for sharing information, it is clear there exists no overarching standard wherein a small to medium sized organization can implement an affordable approach (He et al., 2018).

Current literature seems to indicate there is no effective way to gauge the proper amount or effectiveness of cybersecurity investments. Loonam et al. (2020) opined that cybersecurity and information security do not fully overlap. As such, while information security may be more easily assessed by technical expenditures, because cybersecurity includes concepts such as business intelligence and the work force, identifying effective investment strategies becomes even more challenging (Loonam et al., 2020). Chronopoulos et al. (2018) noted that organizations spend millions of dollars to defend where an attacker's expenditures are trivial. Ultimately, research demonstrates there is still no clear way to effectively ascertain *how much* an

organization should invest in its cybersecurity nor is there a clear method on how to determine *what* to invest in. This impacts everything from physical device acquisition to policy and procedures.

Business Problem Studied

The general problem addressed was the impact of lesser investments in cybersecurity by smaller organizations resulting in a greater susceptibility to organized cyberattacks. Takahashi et al. (2018) stated that one of the primary challenges to organizations is cybersecurity and access to timely and actionable information is critical for thwarting attacks. Chronopoulos et al. (2018) highlighted how organizations are unable to secure their information systems due to ineffective security investment decisions. Fielder et al. (2016) indicated that organizations are unable to effectively invest in resources to combat the threat of attackers due to weak decision-making strategies as related to cybersecurity. The specific problem addressed was the possible failure of leadership within smaller organizations located in southwest Pennsylvania to identify and properly invest in defensive and information sharing systems potentially resulting in data breaches and potentially resulting in the inability to survive long term. Therefore, the study posed three research questions:

RQ1: How has leadership's cybersecurity investment decisions impacted their organization's cybersecurity posture?

RQ2: To what extent have leadership decisions impacted the ability of smaller organizations to respond to high-profile cyber events?

RQ3: How have leadership investment decisions impacted smaller organizations' ability to conduct information sharing amongst operational elements regarding various cyber threat intelligence?

Methodology

The data for the study consisted of mostly qualitative data primarily acquired through employee interviews. While there was some quantitative data collected, the effectiveness of organizational decisions was based on a 'good, better, best' approach and thus presented itself as qualitative in nature. By definition, case study research is most appropriate when the overall intent is to answer the 'how' and 'why' of specific decisions as related to a contemporary event (Villarreal, 2017). Additionally, flexible design is inherently designed to encapsulate the use of qualitative data (Denny & Weckesser, 2019). In this instance, how the organization is impacted by its leadership's decisions and why those decisions are made, aligned with a single case study method. Finally, the use of a single case study created a potential baseline wherein other smaller organizations can be evaluated, especially considering if the organization was successful in its approach or not. Guetterman and Fetters (2018) noted the outcomes of a single case study allow a more effective way to "compare and contrast" (p. 904) the outcomes to other similar organizations.

Triangulation is meant to ensure research is more defensible and credible (Noble & Heale, 2019). Ultimately, this is done to eliminate bias which may be more prevalent in qualitative data, even though it is applicable across both quantitative and qualitative data sets (Campbell et al., 2020; Noble & Heale, 2019). As it is clear this was mostly qualitative data, the employment of bracketing was meant to minimize as much bias as possible in the data, thus the next logical step was to triangulate data for the purpose of a more effective analysis. While there exists various methodologies for data triangulation, the most effective approach in this case was to group findings based on concepts being evaluated.

Racine et al. (2020) demonstrated how data triangulation could be used effectively with both qualitative and quantitative data. By grouping similar concepts from the different datasets and then creating the appropriate protocol for said grouping, they were able to explore any discrepancies/outliers within the data (Racine et al., 2020). As this study's data were derived primarily from in-person interviews using a structured question sheet, it was ideally already organized by 'concept' and thus more easily grouped for triangulation purposes. For example, by collecting quantifiable cost values such as expenditure amounts, the next step was to identify how those figures impacted employee actions. For instance, if it was shown that an employee was unable to share information due to technology limitations, one could review dollar expenditures to determine if the money was allocated and/or spent on the enabling technology. Thus, one can infer that either the expenditure amount was insufficient/non-existent, or the employee did not effectively utilize the technology procured. The culmination of interviews, follow-on written responses, and limited document reviews resulted in an effective approach for capturing the 'ground truth' of the organization.

Data Analysis

Data collection consisted primarily of interviews of both management and operational personnel within the organization. The data ranged from descriptive comments made by participants to simple yes/no responses. The culmination of these disparate data sets required the employment of various techniques ranging from validation of the participants and the accuracy of responses to the proper alignment of data between both research questions and data types. Ruggiano and Perry (2019) discussed the practice of secondary data analysis which could occur thus emphasizing the importance of properly aligning the data from the beginning. They noted how alignment and accuracy of data is pivotal as there exists the potential for follow up

researchers to leverage said data sets to conduct further qualitative reviews (Ruggiano & Perry, 2019).

Although secondary research lends further credibility, the initial organization and coding of the data is pivotal in determining the initial themes (Nepper & Chai, 2016). What was the process for coding and thus determining emerging themes wherein the research questions could best be addressed? To begin, the main themes were divided into three primary categories: information sharing, investments, and posture assessment. As noted, the data were represented in both comment format and simple yes/no responses. In addition, the overall data collection itself was aligned to ensure the data could be collected against each research theme. For example, within each collected data source (e.g., interview, document review, etc.) there existed specific questions which directly fed the researcher's ability to assess the effectiveness of the organization. However, as this was a qualitative approach, the intent was to evaluate the effectiveness based on outside grading and assessments derived from internal participant observations and experiences (Kerr et al., 2010). It became imperative to ensure the totality of relevant data collection was achieved, or as could be stated, data saturation wherein all possible relevant data were collected to the point where additional data had no further bearing on analysis.

How was this accomplished? As Kerr et al. (2010) noted "data for qualitative analyses can also take many forms, including interviews…observations and documentation" (p. 270). These were the primary forms of data collected and all the data collected should have directly mapped to the overarching research questions. But how was the data itself represented? As discussed previously, Appendix A and B represented a more structured approach as to how the interviews occurred. As can be seen, the content was meant to align to each of the research

questions in both an explanatory format and yes/no format. The coding themes of the combined data entry were then based upon the topic areas defined above.

Similar to Nepper and Chai (2016), the data were transcribed and validated for accuracy and then basic exploratory analysis was conducted to identify any emerging themes in the responses. For example, similar statements made by participants were captured and grouped accordingly and from this, the researcher interpreted the theme being presented. As this is an iterative process, it continued until saturation was achieved. In this case, saturation was noted to be synonymous with thematic saturation and as such, could be seen as "data adequacy" or when no further relevant information could be gleaned; it was determined that enough data were collected to achieve this as most answers were fairly synonymous (Kerr et al., 2010, p. 271). The interview portion of data collection compromised a significant portion of the overall data. As such, it was important to accurately capture responses and to ensure they were properly transferred and binned according to the area of focus (See Appendix C and D for summarized data). Some basic quantitative data were required along with the use of basic descriptive statistical analysis, but this was a qualitative study so capturing participant responses was the real key to addressing the research questions.

The primary technique used for triangulation was similar to that demonstrated by Racine et al. (2020). As noted, they grouped findings according to concepts (Racine et al., 2020). In this case, the research questions represented three primary categories of data. Table 1 represents the overall general approach to categorizing data. While the overall approach was that of a qualitative case study, there did exist a need for a few quantifiable metrics such as response rates to some of the yes/no questions. Vetter (2017) noted descriptive statistics can be used to "calculate, describe, and summarize collected research data" (p. 1797).

Once the data were categorized, the data types were reviewed, and the appropriate analysis was applied. For example, there were several questions for all participants related to awareness of recent cyber events. A simple descriptive statistical process showed the percentage of respondents who were aware of these events. From this, one could then glean whether internal information sharing was effective and whether awareness of cyber threats was altering the manner in which the organization operated.

Table 1

Triangulation Categories Based on Research Questions

Category	Theme	Data Source/Type
RQ1	Posture assessment	Interviews with operational/management personnel (qualitative); subsequent written responses (qualitative/quantitative)
RQ2	Information sharing	Interviews with operational personnel (qualitative); subsequent written responses (qualitative/quantitative); document existence review (quantitative)
RQ3	Investments	Interviews with operational/management personnel (qualitative); subsequent written responses (qualitative/quantitative); document existence review (quantitative)

Findings

Analysis of the data showed that although the participant organization was indeed a smaller organization with both limited budget and personnel, it had not been successfully breached within the past 24 months. There was no mention of ever having been breached, despite its critical role in helping to combat cybercrime. From this data gathering and analysis, four themes were derived wherein a smaller organization could potentially review the actions taken by the organization, and where possible, mirror those actions. Those themes were:

1. A smaller organization secured itself despite limited resources.

2. An organization which kept employees informed of IT/security issues had more buy-in regarding the importance of maintaining a secure environment.
3. An involved IT team with the daily operations of the organization created trust in the capability of the IT team, thus translating into the organization perceiving itself as highly capable regarding cyber threats.
4. A smaller organization employed mechanisms either through policy or IT solutions wherein information was effectively exchanged with external organizations.

The four themes are all indicative that organizations, despite their size, can be effective in their security approach. This is centered on the notion that the organization was fundamentally committed to its security. Regardless of their role, the overarching number of participants in the various discussions were able to identify key policies and acquisitions which were critical to the organization's security.

Christian Perspective on the Business Problem and Findings

When one thinks of the Christian worldview, it can be difficult to determine if there is a connection with the 'things of this world' and that of God's purpose. Is there truly a connection between the Christian worldview and a study involving information sharing and leadership decisions, as related to cyber threats? One can argue there exists no connection. However, the Bible is clear in that we are to acquire knowledge because "an intelligent heart acquires knowledge, and the ear of the wise seeks knowledge" (*English Standard Version*, 2001, Proverbs 18:15). Therefore, it becomes immediately clear there exists almost no endeavor in which we cannot seek to align its purpose with acquiring knowledge, but more importantly, doing so for the purpose of serving the Lord. For example, in this study, the intent was to determine the impact of leadership decisions on a small organization. With leadership being the operative

word, irrespective of the organization, the Bible states that we are to ensure that those we serve possess certain characteristics. In the book of Exodus it is written “moreover, look for able men from all the people, men who fear God, who are trustworthy and hate a bribe, and place such men over the people as chiefs of thousands, of hundreds, of fifties, and of tens” (*English Standard Version*, 2001, Exodus 18:21). Therefore, one can argue an effective leader will have certain qualities, specifically those of good moral character. So, can a truly effective leader, especially in a smaller organization, be an immoral, untrusted person? Can an organization have an employee base which is overwhelmingly positive and supportive of said leadership if the leadership does not possess good moral character? Again, it becomes clear there does exist a relationship between the success of an organization and the type of leadership it possesses and thus a direct correlation to the Christian worldview. In this study, it was shown that leadership provided a strategic direction in the form of policies and investment decisions, and in addition, the employee base was supportive of said decisions. It can be said, “the plans of the diligent lead surely to abundance, but everyone who is hasty comes only to poverty” (*English Standard Version*, 2001, Proverbs 21:5).

Another biblical principle which is directly related to the study is that of watchfulness. Both small- and mid-sized organizations seem to bear the brunt of cyberattacks and as such, must remain ever vigilant. This study evaluated the effectiveness of a smaller organization and determined that it had made effective decisions in its approach to security. This is aligned with biblical principles because the Bible specifically warns us to “be sober-minded; be watchful. Your adversary the devil prowls around like a roaring lion, seeking someone to devour” (*English Standard Version*, 2001, 1 Peter 5:8). While this is referring to our souls, the principle is nonetheless extremely relevant as adversaries targeting organizations do not represent the

betterment of society. The adversaries look to steal, damage, or simply stated, inflict pain on their victims. The principle of watchfulness is important in both a personal and professional sense and thus evaluating this organization is in essence a measure of its watchfulness.

What can be seen as something advised merely for those who believe, seems to provide a wisdom that any organization can follow. The study correlates how biblical principles, while not necessarily overtly stated in the organization, do provide a strength and knowledge that will better ensure the survivability of the organization. The Christian worldview is predicated upon biblical principles wherein those of faith seek to be drawn closer to the Lord, but even those who do not seek the counsel of the Lord, can be ascertained successful or not merely by how well their actions align with what has been shown 'correct' for millennium.

Conclusion

The study addressed the challenge that many smaller organizations have, specifically, does there exist investment approaches and information strategies wherein an organization, with limited resources, can still secure itself. Researchers were very clear, smaller organizations struggle to defend against cyberattacks, primarily due to limited resources and personnel (Raineri & Fudge, 2019). While the focus was on investment and information sharing, the core component which ultimately drove the success of the organization was leadership and its commitment to the idea of creating a culture wherein security was a cornerstone principle. The study highlighted multiple challenges, but ultimately, with 73% of breaches occurring within small- to mid-size organizations, it is clear the organization reviewed was likely to have at least been targeted (Fielder et al., 2016).

The study consisted of a qualitative approach wherein various personnel from a smaller organization located in southwest Pennsylvania were interviewed over a 2-week period. The

participants ranged from junior analysts up to the president. The questions ranged from mere assessments of the awareness of various policies to specific questions regarding organizational investments and actions taken in response to well-known cyber events. During this process, it was discovered fairly early that the organization, while limited in number of IT personnel directly responsible for the security of the organization, had not suffered a successful cyberattack in the past 24 months. Furthermore, as was shown in the analysis, the overall awareness of cyber threats and the organization's ability to send and receive information was rated fairly high. Therefore, the organization also did not neglect their duty to spend for security and/or IT purchases. While the organization did not have an endless budget, leadership was very clear in that security was a priority and investment and actions would reflect that.

This study makes it clear that a smaller organization can defend itself from cyber threat actors. The success of this organization resided in its leadership's commitment to inform its employees of the ongoing nature of the threats they face. Furthermore, leadership was willing to invest as able. As advanced persistent threat actors continue to grow, for an organization to think it does not need to invest in security is ludicrous. However, there still exists no clear metric for determining the optimum amount for each organization. In the end, this is where organizational needs and risk-based approaches may need to ultimately be the driving forces and as such, it is quite possible there will be no uniform approach or metric for cyber security investing. But regardless, the key intangible was that employee awareness coupled with leadership's determination to infuse a culture of security did ultimately pave the way for investments, training, information sharing, and other steps taken wherein the end result was no breaches in the past 24 months.

References

Campbell, R., Goodman-Williams, R., Feeney, H., & Fehler-Cabral, G. (2020). Assessing triangulation across methodologies, methods, and stakeholder groups: The joys, woes, and politics of interpreting convergent and divergent data. *The American Journal of Evaluation*, *41*(1), 125–144. https://doi.org/10.1177/1098214018804195

Chronopoulos, M., Panaousis, E., & Grossklags, J. (2018). An options approach to cybersecurity investment. *IEEE Access*, *6*, 12175–12186. https://doi.org/10.1109/ACCESS.2017.2773366

Denny, E., & Weckesser, A. (2019). Qualitative research: What it is and what it is not: Study design: Qualitative research. *BJOG: An International Journal of Obstetrics and Gynaecology*, *126*(3), 369–369. https://doi.org/10.1111/1471-0528.15198

English Standard Version. (2001). ESV Online. https://esv.literalword.com

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cybersecurity investment. *Decision Support Systems*, *86*, 13–23. https://doi.org/10.1016/j.dss.2016.02.012

Garg, P. (2020). Cybersecurity breaches and cash holdings: Spillover effect. *Financial Management*, *49*(2), 503–519. https://doi.org/10.1111/fima.12274

Guetterman, T. C., & Fetters, M. D. (2018). Two methodological approaches to the integration of mixed methods and case study designs: A systematic review. *The American Behavioral Scientist (Beverly Hills)*, *62*(7), 900–918. https://doi.org/10.1177/0002764218772641

He, M., Devine, L., & Zhuang, J. (2018). Perspectives on cybersecurity information sharing among multiple stakeholders using a decision-theoretic approach. *Risk Analysis*, *38*(2), 215–225. https://doi.org/10.1111/risa.12878

Kerr, C., Nixon, A., & Wild, D. (2010). Assessing and demonstrating data saturation in qualitative inquiry supporting patient-reported outcomes research. *Expert Review of Pharmacoeconomics & Outcomes Research*, *10*(3), 269–281. https://doi.org/10.1586/erp.10.30

Loonam, J., Zwiegelaar, J., Kumar, V., & Booth, C. (2020). Cyber-resiliency for digital enterprises: A strategic leadership perspective. *IEEE Transactions on Engineering Management*, *69*(6), 3757–3770. https://doi.org/10.1109/TEM.2020.2996175

Nepper, M. J., & Chai, W. (2016). Parents' barriers and strategies to promote healthy eating among school-age children. *Appetite*, *103*, 157–164. https://doi.org/10.1016/j.appet.2016.04.012

Noble, H., & Heale, R. (2019). Triangulation in research, with examples. *Evidence Based Nursing*, *22*(3), 67–68. https://doi.org/10.1136/ebnurs-2019-103145

Racine, E., Riordan, F., Phillip, E., Flynn, G., McHugh, S., & Kearney, P. M. (2020). It just wasn't going to be heard': A mixed methods study to compare different ways of involving people with diabetes and health-care professionals in health intervention research. *Health Expectations: An International Journal of Public Participation in Health Care and Health Policy*, *23*(4), 870–883. https://doi.org/10.1111/hex.13061

Raineri, E. M., & Fudge, T. (2019). Exploring the sufficiency of undergraduate students' cybersecurity knowledge within top universities' entrepreneurship programs. *Journal of Higher Education Theory and Practice*, *19*(4), 73–92. https://doi.org/10.33423/jhetp.v19i4.2203

Ruggiano, N., & Perry, T. E. (2019). Conducting secondary analysis of qualitative data: Should we, can we, and how? *Qualitative Social Work: QSW: Research and Practice*, *18*(1), 81–97. https://doi.org/10.1177/1473325017700701

Takahashi, T., Panta, B., Kadobayashi, Y., & Nakao, K. (2018). Web of cybersecurity: Linking, locating, and discovering structured cybersecurity information. *International Journal of Communication Systems*, *31*(3), e3470–e3490. https://doi.org/10.1002/dac.3470

Vetter, T. R. (2017). Descriptive statistics: Reporting the answers to the 5 basic questions of who, what, why, when, where, and a sixth, so what? *Anesthesia and Analgesia*, *125*(5), 1797–1802. https://doi.org/10.1213/ANE.0000000000002471

Villarreal, O. (2017). Is it desirable, necessary and possible to perform research using case studies? *Cuadernos De gestión*, *17*(1), 147–172. https://doi.org/10.5295/cdg.140516ov